

REMARKS

Claims 1 - 10 are pending in the present application. Applicant amended claims 1 and 7 - 10 to further clarify the invention. Applicant refers to Fig. 2 and page 14, lines 10 - 21 of the specification for support of said claim amendments. Applicant also amended claim 3 to correct a minor error. No new matter has been added.

Claims 1 - 6 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. In particular, the Examiner objected to the phrase "public/secret keys" as being unclear. Applicant amended the claims to replace this phrase with "public and secret keys," and respectfully requests that the Examiner withdraw the §112, ¶2 rejection.

Claim 10 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,373,950 to Rowney; claims 1-2 and 4-9 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Rowney in view of U.S. Patent No. 6,732,269 to Baskey et al. and further in view of "Handbook of Applied Cryptography" by Menezes et al.; and claim 3 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Rowney, Baskey et al., Menezes et al., and further in view of U.S. Patent No. 6,351,813 to Mooney et al. Applicant amended independent claims 1 and 7-10 in a good faith effort to further clarify the invention as distinguished from the cited art, and, therefore, respectfully traverses the rejections.

Rowney, as applied by the Examiner, describes a transaction authorization scheme using secure transmission of data from a customer computer system to a merchant computer system, which, in turn, transmits payment information to a payment gateway computer system where the transaction is authorized using a host legacy system. Col. 4, lines 40-63 of Rowney. The

Examiner acknowledged that Rowney does not disclose "the proxy server being provided between a user terminal and an electronic market server and the shared key being a common key," (page 5, lines 17-19 of the Office Action) but relied upon Baskey et al. as a combining reference for disclosing a proxy server between a client and a server, and relied upon Menezes et al. as a further combining reference for disclosing a common key. The cited portions of Baskey et al., col. 5, lines 17-37, merely describe an SSL proxy server operable in routing client specific SSL connections onto a persistent secure connection between the SSL proxy server and a transaction server. And the cited portions of Menezes et al., page 15, provide an overview of symmetric-key encryption (also known as single-key, one-key, private key, and conventional encryption).

It is, therefore, respectfully submitted that even assuming, arguendo, that it would be obvious to one skilled in the art to combine Rowney, Baskey et al., and Menezes et al. in the manner proposed by the Examiner, such combination would still fail to teach or suggest,

"a proxy means for executing authentication of a certificate and exchanging a common key X between the proxy server and the electronic market server, using public and secret keys of the electronic market server; and
an informing means for informing the common key X to the user terminal through the encrypted communication session, which common key X is encrypted by using a common key X' that was exchanged between the user terminal and the proxy server;

wherein an encrypted communication is executed directly between the user terminal and the electronic market server by using the common key X that was exchanged between the proxy server and the electronic market server," as recited in claim 1. (Emphasis added)

Accordingly, applicant respectfully submits that independent claim 1, together with claims 2 and 4-6 dependent therefrom, is patentable over Rowney, Baskey et al., and Menezes et al. individually and in combination. Independent claims 7-10 have been amended to include

limitations similar to those discussed above from claim 1, and are, therefore, patentable over the cited art for at least the same reasons.

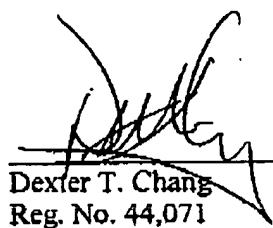
With respect to dependent claim 3, the Examiner relied upon Mooney et al. to describe specifically the additional limitations thereof. The cited portions of Mooney et al., col. 1, lines 59-67, col. 2, lines 1-11, and col. 9, lines 31-36, describe the use of a smart card for access control, the use of a secret password for decrypting encrypted data transferred from a first site to a second site, and the use of a second password or biometric information to generate an encryption key. They do not teach or suggest the above recited features of claim 1. Applicant, therefore, respectfully submits that the combination of Mooney et al. with Rowney, Baskey et al., and Menezes et al. in the manner proposed by the Examiner does not teach or suggest the above features of claim 1 that are incorporated in dependent claim 3, even assuming such a combination would be obvious to one skilled in the art. Accordingly, applicant submits that claim 3 is patentable over Rowney, Baskey et al., Menezes et al., and Mooney et al..

Statements appearing above in respect to the disclosures in the cited references represent the present opinions of the undersigned attorney and, in the event that the Examiner disagrees with any of such opinions, it is respectfully requested that the Examiner specifically indicate those portions of the respective reference providing the basis for a contrary view.

In view of the remarks set forth above, this application is in condition for allowance which action is respectfully requested. However, if for any reason the Examiner should consider this application not to be in condition for allowance, the Examiner is respectfully requested to telephone the undersigned attorney at the number listed below prior to issuing a further Action.

Any fee due with this paper may be charged to Deposit Account No. 50-1290.

Respectfully submitted,



Dexter T. Chang
Reg. No. 44,071

CUSTOMER NUMBER 026304
Telephone: (212) 940-6384
Fax: (212) 940-8986 or 8987
Docket No.: 100794-11683 (FUJA 18.570)
DTC:fd